LAW OFFICE OF FRANCIS J. FLYNN, JR.
Francis J. "Casey" Flynn, Jr. (SBN 304712)
6057 Metropolitan Plz.
Los Angeles, California 90036
Telephone: (314) 662-2836
Email: casey@lawofficeflynn.com

LAW OFFICE OF PAUL C. WHALEN, P.C.
Paul C. Whalen (*pro hac vice forthcoming*)
768 Plandome Road
Manhasset, NY 11030
Telephone: (516) 426-6870
Email: paul@paulwhalen.com

Counsel for Plaintiff and the Proposed Classes

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

MELISSA RYAN, individually and on behalf of all others similarly situated,

Plaintiffs,

vs.

LOANDEPOT, INC.,

Defendant.

Case No.: 2:24-cv-3630

COMPLAINT FOR DAMAGES AND INJUNCTIVE RELIEF FOR:

1. Negligence
3. Violation of Unfair Competition Law, California Business and Professional Code Section 17200, et seq.
4. Violation of California Customer Records Act, California Civil Code § 1798.80 et. seq.
5. Breach of Contract
6. Unjust Enrichment
7. Invasion of Privacy
8. Breach of Implied Contract
9. Breach of Fiduciary Duty
10. Injunctive/Declaratory Relief

FOR INJUNCTIVE RELIEF ONLY FOR:

2. Violation of California Consumers Legal Remedies Act, California Civil Code § 1750, et seq.

CLASS ACTION

DEMAND FOR JURY TRIAL

Plaintiff Melissa Ryan ("Plaintiff"), individually, and on behalf of the class defined below, by and through Plaintiff's undersigned counsel, brings this class action complaint against loanDepot, Inc. ("loanDepot" or "Defendant") and, based upon information and belief and the investigation of Plaintiff's counsel, alleges as follows:

STATEMENT OF JURISDICTION

1. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00, exclusive of interest and costs, there are 100 or more members of the proposed class, and at least one member of the proposed class, including Plaintiff, is a citizen of a state different than Defendant.

2. This Court has personal jurisdiction over Defendant because Defendant conducts business in California, including within this District. Defendant is headquartered in Irvine, California and, therefore, has sufficient minimum contacts with this state, and/or sufficiently avail themselves to the markets of this state through their sales and marketing within this state to render the exercise of jurisdiction by this Court permissible.

3. Under 28 U.S.C. 1391, venue lies in this District because Defendant is headquartered in this District and makes decisions regarding its privacy practices from its headquarters and are thus subject to the court's personal jurisdiction as indicated more fully below. A Venue affidavit is attached hereto as **Exhibit A**.

INTRODUCTION

4. Defendant loanDepot, Inc. is a nonbank holding company based out of Irvine, California, which sells mortgage and non-mortgage lending products. Founded in 2010, loanDepot has "grown to become the nation's fifth largest retail mortgage lender and the second largest nonbank retail originator, funding more than $275 billion since inception. Today, [loanDepot's] nationwide team of 6,000-plus members

assists more than 27,000 customers each month."[1]

5. Between January 8, 2024 and January 22, 2024, loanDepot announced a security incident during which unauthorized parties gained access to sensitive personal information of approximately 16.6 million individuals in its systems (the "Data Breach").

6. Specifically, on or around January 8, 2024, in a Form 8-K filing[2] with the SEC, loanDepot reported the following:

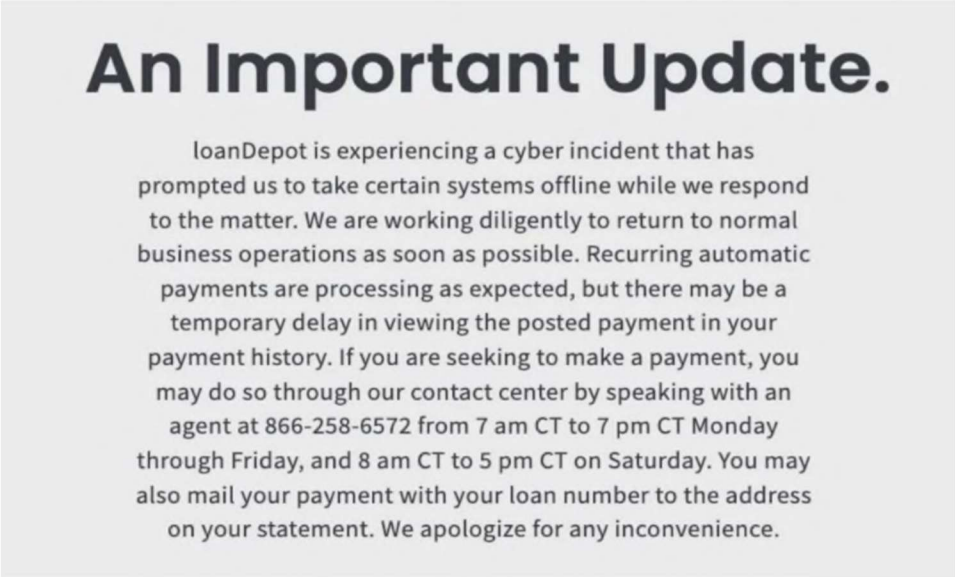
> loanDepot, Inc. (the "Company") recently identified a cybersecurity incident affecting certain of the Company's systems. Upon detecting unauthorized activity, the Company promptly took steps to contain and respond to the incident, including launching an investigation with assistance from leading cybersecurity experts, and began the process of notifying applicable regulators and law enforcement.
>
> Though our investigation is ongoing, at this time, the Company has determined that the unauthorized third party activity included access to certain Company systems and the encryption of data. In response, the Company shut down certain systems and continues to implement measures to secure its business operations, bring systems back online and respond to the incident.[3]

7. On or around January 8, 2024, loanDepot also announced the following on its website: loanDepot is experiencing a cyber incident. We have taken certain systems offline and are working diligently to restore normal business operations as quickly as possible. We are working quickly to understand the extent of the incident and taking steps to minimize its impact. The Company has retained leading forensics experts to aid in our investigation and is working with law enforcement. We sincerely apologize for any impacts to our customers and we are focused on resolving these

[1] https://www.loandepot.com/about
[2] *See* https://investors.loandepot.com/financials/sec-filings/default.aspx
[3] *See* loanDepot January 8, 2024 Form 8-K Filing, https://d18rn0p25nwr6d.cloudfront.net/CIK-0001831631/446c437f-153f-425d-adc6-bf37155d6e91.pdf (last accessed January 23, 2024).

matters as soon as possible.[4]

8. Around this time, loanDepot's website, including its customer portals, appeared to be non-functional, and the following error message appeared on loanDepot's customer login page, asking customers seeking to make a payment to call or mail in their payment instead:[5]



9. On January 22, 2024, in a Form 8-K/A filing[6] with the SEC, loanDepot further reported, "[T]he Company has determined that an unauthorized third party gained access to sensitive personal information of approximately 16.6 million individuals in its systems. The Company will notify these individuals and offer credit monitoring and identity protection services at no cost to them."

10. On January 22, 2024, loanDepot also provided the following information on its website:

---

[4] *See* loanDepot, *loanDepot is experiencing a cyber incident*, https://loandepot.cyberincidentupdate.com/ (last accessed Jan. 23, 2024).

[5] https://techcrunch.com/2024/01/08/loandepot-outage-suspected-ransomware-attack

[6] *See* loanDepot Form 8:K/A Filing; https://d18rn0p25nwr6d.cloudfront.net/CIK-0001831631/80bb5ce4-2f0e-49d6-b1a1-bd5aa864f4d1.pdf (last accessed Jan. 23, 2024).

> The Company has been working diligently with outside forensics and security experts to investigate the incident and restore normal operations as quickly as possible. The Company has made significant progress in restoring our loan origination and loan servicing systems, including our MyloanDepot and Servicing customer portals.
>
> Although its investigation is ongoing, the Company has determined that an unauthorized third party gained access to sensitive personal information of approximately 16.6 million individuals in its systems. The Company will notify these individuals and offer credit monitoring and identity protection services at no cost to them.[7]

11. According to the Notice of Data Breach:

> **What Happened?**
>
> […] Through our investigation of the incident, we determined that between January 3rd and January 5th, 2024 an unauthorized thirdp arty gained access to certain of our systems, including certain senstivie personal information stored in those systems.
>
> **What Information Was Involved?**
>
> The incident may have impacted your name, address, email address, financial account numbers, social security number, phone number, and date of birth.

See, **Exhibit B**, Notice of Data Breach at 1.

12. At all relevant times, Defendant was aware of the risks of a Data Breach and that it would be specifically targeted by malicious hackers. Defendant's CEO Frank Martel acknowledged as much, stating, "Unfortunately, we live in a world where these types of attacks are increasingly frequent and sophisticated, and our industry has not been spared. We sincerely regret any impact to our customers."[8]

---

[7] *See* loanDepot, *loanDepot Provides Update on Cuber Incident,* https://media.loandepot.com/news-releases/press-release-details/2024/loanDepot-Provides-Update-on-Cyber-Incident/default.aspx (last accessed Jan. 23, 2024).

[8] *See*, *supra*, n. 7.

loanDepot also suffered another data security incident in August 2022 (which it did not announced until May 2023) whereby unauthorized parties accessed documents containing its customers' personal information.[9]

13. Armed with the PII from these records, hackers can sell the PII to other thieves or misuse themselves to commit a variety of crimes that harm victims of the Data Breach. For instance, they can take out loans, mortgage property, open financial accounts, and open credit cards in a victim's name; use a victim's information to obtain government benefits or file fraudulent returns to obtain a tax refund; obtain a driver's license or identification card in a victim's name; gain employment in another person's name; or give false information to police during an arrest.

14. As a result of Defendant's willful failure to prevent the Data Breach, Plaintiff and Class members are more susceptible to identity theft and have experienced, will continue to experience, and face an increased risk of financial harms, in that they are at substantial risk of identity theft, fraud, and other harm.

PARTIES

15. Plaintiff Melissa Ryan is a resident and citizen of San Diego County, California. Plaintiff applied for and obtained a personal loan from loanDepot on or about May 2022. Plaintiff applied for and obtained one or more loans prior to May 2022 as well. Through this application, Plaintiff provided Defendant her PII. Plaintiff received a notice of Data Breach on or about February 23, 2024, informing Plaintiff of a data security incident which compromised loan Depot's systems, which contained Plaintiff's PII. A copy[10] of the Notice of Data Breach is attached hereto as **Exhibit B**. Plaintiff has not knowingly sent PII to third parties in a non-encrypted manner. Since the breach, Plaintiff has received more spam calls since the Data Breach.

16. As a result of Defendant's actions, Plaintiff has been injured and has

[9] https://www.mass.gov/doc/assigned-data-breach-number-29545-loandepotinc/download.

[10] Plaintiff's PII has been redacted from **Exhibit B**.

financial losses and will be subject to a substantial risk for further identity theft due to Defendant's Data Breach. As a further result of Defendant's actions, Plaintiff will need to purchase credit monitoring and take other measures to protect herself from identity theft and fraud. Plaintiff believed, at the time of applying for her personal loan, that loanDepot would maintain the privacy and security of the PII she provided to it. Plaintiff further believes she paid a premium to loanDepot for its data security. Plaintiff would not have used loanDepot had she known that it would expose sensitive PII, making her available to identity thieves.

17. Defendant loanDepot, Inc. is a Delaware corporation with its principal place of business in Irvine, California.

FACTUAL ALLEGATIONS

A. The Data Breach

18. Defendant loanDepot, Inc. is an Irvine, California-based nonbank holding company which sells mortgage and non-mortgage lending products. Founded in 2010, loanDepot has "grown to become the nation's fifth largest retail mortgage lender and the second largest nonbank retail originator, funding more than $275 billion since inception. Today, [loanDepot's] nationwide team of 6,000-plus members assists more than 27,000 customers each month."

19. Customers believe that—at a minimum—the large sum they pay for a mortgage loan buys them security and peace of mind that their sensitive information will be securely stored.

20. In its Privacy Policy, loanDepot makes numerous promises to its customers that it will maintain the security and privacy of their personal information. For instance, loanDepot states the following in its Privacy Policy:

> loanDepot® values your patronage and protecting your personal information is a priority. loanDepot believes in protecting the confidentiality and security of the information we collect about you as a customer, potential customer, former customer, job applicant, or employee. We have adopted the following policies and procedures to

safeguard the personal information about you in our possession.[11]

21. The Privacy Policy also provides that Defendant collects the following information on its customers:

- Identifying information, such as your name, age, address, phone number and social security number
- Employment information
- Contact information (such as first and last name, mailing or property address, phone number, email address)
- Account access information, such as username and password
- Demographic information (such as date of birth, gender, marital status, ethnicity, race)
- Social security, driver's license, passport, and other government identification numbers
- Loan account information (such as loan number)
- Bank account and credit/debit card numbers
- Other personal information needed from you to provide real estaterelated, loan-related, insurance-related, credit-related, and homeownership-related services to you
- Information for fraud detection and prevention
- Financial information such as your income, assets and liabilities, as well as information about your savings, investments, insurance and business.[12]

22. In a section entitled, "Safeguarding Personally Identifiable Information," loanDepot provides the following assurances to its customers:

- We have adopted policies and procedures designed to protect your personally identifiable information from unauthorized use or disclosure.

[11] loanDepot, Privacy Policy, https://www.loandepot.com/privacypolicy (last accessed Jan. 23, 2024).
[12] *Id.*

- We have implemented physical, electronic, and procedural safeguards to maintain confidentiality and integrity of the personal information in our possession and to guard against unauthorized access. These include among other things, procedures for controlling access to your files, building security programs and information technology security measures such as the use of passwords, firewalls, virus prevention and use detection software.
- We continue to assess new technology as it becomes available and to upgrade our physical and electronic security systems as appropriate.
- Our policy is to permit employees to access your personal information only if they have a business purpose for using such information, such as administering, providing or developing our products or services.
- Our policy, which governs the conduct of all of our employees, requires all employees to safeguard personally identifiable information about the consumers and customers we serve or have served in the past.[13]

23. The Privacy Policy also has a section entitled, "loanDepot Security Policy," which provides the following:

> loanDepot takes steps to safeguard your personal and sensitive information through industry standard physical, electronic, and operational policies and practices. All data that is considered highly confidential data can only be read or written through defined service access points, the use of which is password protected. The physical security of the data is achieved through a combination of network firewalls and servers with tested operating systems, all housed in a secure facility. Access to the system, both physical and electronic, is controlled and sanctioned by a highranking manager.[14]

24. Despite all of these promises, on January 8, 2024, loanDepot allowed the Data Breach to occur whereby the personal, confidential PII of Plaintiff and Class members were viewed, disclosed to, and acquired by unauthorized parties. The Data

[13] *Id.*
[14] *Id.*

Breach exposed the sensitive PII and financial information of approximately 16.6 million customers.

B. Personally Identifiable Information ("PII")

25. PII is of great value to hackers and cyber criminals and the data compromised in the Data Breach can be used in a variety of unlawful manners.

26. PII is information that can be used to distinguish, identify, or trace an individual's identity, such as their name, Social Security number, and biometric records. This can be accomplished alone, or in combination with other personal or identifying information that is connected, or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.

27. PII does not include only data that can be used to directly identify or contact an individual (e.g., name, e-mail address), or personal data that is especially sensitive (e.g., Social Security number, bank account number, payment card numbers).

28. Given the nature of the Data Breach, it is foreseeable that the compromised PII will be used to access Plaintiff and the Class members' financial accounts, thereby providing access to additional PII or personal and sensitive information. Therefore, the compromised PII in the Data Breach is of great value to hackers and thieves and can be used in a variety of ways. Information about, or related to, an individual for which there is a possibility of logical association with other information is of great value to hackers and thieves. Indeed, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[15] For example, different

[15] Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report 35-38 (Dec. 2010) <https://www.ftc.gov/sites/default/files/documents/reports/federaltrade-

PII elements from various sources may be able to be linked in order to identify an individual, or access additional information about or relating to the individual.

29. Further, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."[16]

30. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts particularly when they have easily-decrypted passwords and security questions.

31. The PII loanDepot exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breach can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names.

32. Unfortunately for Plaintiff and Class members, a person whose PII has been compromised may not fully experience the effects of the breach for years to come:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[17]

---

commission-bureau-consumer-protection-preliminary-ftc-staff-reportprotecting-consumer/101201privacyreport.pdf> [as of June 24, 2017]

[16] Fed. Chief Information Officers Council, Recommendations for Standardized Implementation of Digital Privacy Controls (Dec. 2012) pp. 7-8.

[17] G.A.O., Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown (June 2007) <http://www.gao.gov/assets/270/262904.html.> [as of June 24, 2017].

33. Accordingly, Plaintiff and Class members will bear a heightened risk of injury for years to come. Identity theft is one such risk and occurs when an individuals' PII is used without his or her permission to commit fraud or other crimes.[18]

34. According to the Federal Trade Commission, "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data."[19]

35. To make matter worse, in 2017, the FBI warned the real estate industry of a "large spike in cyberattacks specifically targeting real estate companies." The FBI said that between 2016 and 2017, it witnessed a 480% increase in cyberattacks on the real estate industry.

36. loanDepot ignored these warnings and risks and failed to invest in sufficient privacy and security protections.

37. At all relevant times, Defendant was aware of the risks of a Data Breach and that it would be specifically targeted by malicious hackers. Defendant's CEO Frank Martel acknowledged as much, stating, "Unfortunately, we live in a world where these types of attacks are increasingly frequent and sophisticated, and our industry has not been spared. We sincerely regret any impact to our customers."[20] loanDepot also suffered another data security incident in August 2022 (which it did not announced until May 2023) whereby unauthorized parties accessed documents

---

[18] Fed. Trade Comm'n, Taking Charge: What To Do If Your Identity Is Stolen (April 2013) <https://www.consumer.ftc.gov/articles/pdf-0014-identity-theft.pdf> [as of June 24, 2017].

[19] Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change (March 2012) <https://www.ftc.gov/sites/default/files/documents/reports/federaltrade-commission-report-protecting-consumer-privacy-era-rapid-changerecommendations/ 120326privacyreport.pdf> [as of June 24, 2017].

[20] *See*, *supra*, n. 7.

containing its customers' personal information.[21]

38. As a direct and proximate result of loanDepot's reckless and negligent actions, inaction, and omissions, the resulting Data Breach, the unauthorized release and disclosure of Plaintiff's and Class members' PII, and loanDepot's failure to properly and timely notify Plaintiff and Class members, Plaintiff and Class members are more susceptible to identity theft and have experienced, will continue to experience and will face an increased risk of experiencing the following injuries, *inter alia*:

a. money and time expended to prevent, detect, contest, and repair identity theft, fraud, and/or other unauthorized uses of personal information;

b. money and time lost as a result of fraudulent access to and use of their financial accounts;

c. loss of use of and access to their financial accounts and/or credit;

d. money and time expended to avail themselves of assets and/or credit frozen or flagged due to misuse;

e. impairment of their credit scores, ability to borrow, and/or ability to obtain credit;

f. lowered credit scores resulting from credit inquiries following fraudulent activities;

g. money, including fees charged in some states, and time spent placing fraud alerts and security freezes on their credit records;

h. costs and lost time obtaining credit reports in order to monitor their credit records;

i. anticipated future costs from the purchase of credit monitoring and/or identity theft protection services;

[21] https://www.mass.gov/doc/assigned-data-breach-number-29545-loandepotinc/download.

j. costs and lost time from dealing with administrative consequences of the Data Breach, including by identifying, disputing, and seeking reimbursement for fraudulent activity, canceling compromised financial accounts and associated payment cards, and investigating options for credit monitoring and identity theft protection services;

k. money and time expended to ameliorate the consequences of the filing of fraudulent tax returns;

l. lost opportunity costs and loss of productivity from efforts to mitigate and address the adverse effects of the Data Breach including, but not limited to, efforts to research how to prevent, detect, contest, and recover from misuse of their personal information;

m. loss of the opportunity to control how their personal information is used; and

n. continuing risks to their personal information, which remains subject to further harmful exposure and theft as long as loanDepot fails to undertake appropriate, legally required steps to protect the personal information in its possession.

39. The risks associated with identity theft are serious. "While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit."[22]

40. Further, criminals often trade stolen PII on the "cyber black-market" for years following a breach. Cybercriminals can post stolen PII on the internet, thereby making such information publicly available.

[22] True Identity Protection: Identity Theft Overview, ID Watchdog <http://www.idwatchdog.com/tikia//pdfs/Identity-Theft-Overview.pdf> [as of Sept. 23, 2016].

CHOICE OF LAW ALLEGATIONS

41. The State of California has sufficient contacts regarding the conduct at issue in this Complaint, such that California law may be uniformly applied to the claims of the proposed Class.

42. Defendant does substantial business in California; their headquarters is located in California; and a significant portion of the proposed Nationwide Class is located in California.

43. In addition, the conduct that forms the basis for each and every Class member's claims against loanDepot emanated from Defendant's headquarters in Irvine, California.

44. The State of California also has the greatest interest in applying its law to Class members' claims. California's governmental interests include not only compensating resident consumers under its consumer protection laws, but also what the State has characterized as a "compelling" interest in using its laws to regulate a resident corporation and preserve a business climate free of unfair and deceptive practices. *Diamond Multimedia Sys. v. Sup. Ct*., 19 Cal. 4th 1036, 1064 (1999).

45. If other states' laws were applied to Class Members' claims, California's interest in discouraging resident corporations from engaging in the sort of unfair and deceptive practices alleged in this complaint would be significantly impaired. California could not effectively regulate a company like loanDepot, which does business throughout the United States, if it can only ensure remuneration for consumers from one of the fifty states affected by conduct that runs afoul of its laws.

CLASS ACTION ALLEGATIONS

46. Plaintiff brings all claims as class claims under Federal Rule of Civil Procedure 23(b)(1), (b)(2), (b)(3), and (c)(4).

A. Nationwide Class

47. Plaintiff brings all claims on behalf of a proposed nationwide class ("Nationwide Class"), defined as follows:

All persons who utilized loanDepot, Inc.'s title insurance, homeowner's insurance, mortgages, refinancing, home warranties, or other closing services provided by loanDepot, Inc.

48. **Numerosity:** The Nationwide Class is so numerous that joinder of all members is impracticable. Based on information and belief, the Nationwide Class includes millions of individuals from across the country who has their PII compromised, stolen, and published during the Data Breach. The parties will be able to identify the exact size of the class through discovery and loanDepot's own documents.

49. **Commonality:** There are numerous questions of law and fact common to Plaintiff and the Nationwide Class including, but not limited to, the following:

(a) whether Defendant engaged in the wrongful conduct alleged herein;

(b) whether Defendant owed a duty to Plaintiff and members of the Nationwide Class to adequately protect their personal information;

(c) whether Defendant breached their duties to protect the personal information of Plaintiff and Nationwide Class members;

(d) whether Defendant knew or should have known that its data security systems, policies, procedures, and practices were vulnerable;

(e) whether Plaintiff and Nationwide Class members suffered legally cognizable damages as a result of Defendant's conduct, including increased risk of identity theft and loss of value of PII;

(f) whether Defendant violated state consumer protection statutes; and

(g) whether Plaintiff and Nationwide Class members are entitled to equitable relief including injunctive relief.

50. **Typicality:** Plaintiff's claims are typical of the claims of the Nationwide Class members. Plaintiff, like all proposed Nationwide Class members, had their personal information compromised in the Data Breach.

51. **Adequacy:** Plaintiff will fairly and adequately protect the interests of the

Nationwide Class. Plaintiff has no interests that are averse to, or in conflict with, the Nationwide Class members. There are no claims or defenses that are unique to Plaintiff. Likewise, Plaintiff has retained counsel experienced in class action and complex litigation, including data breach litigation, and have sufficient resources to prosecute this action vigorously.

52. **Predominance:** The proposed action meets the requirements of Federal Rule of Civil Procedure 23(b)(3) because questions of law and fact common to the Nationwide Class predominate over any questions which may affect only individual Nationwide Class members.

53. **Superiority:** The proposed action also meets the requirements of Federal Rule of Civil Procedure 23(b)(3) because a class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions is superior to multiple individual actions or piecemeal litigation, avoids inconsistent decisions, presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each class member.

54. Absent a class action, the majority Nationwide Class members would find the cost of litigating their claims prohibitively high and would have no effective remedy.

55. **Risks of Prosecuting Separate Actions:** Plaintiff's claims also meet the requirements of Federal Rule of Civil Procedure 23(b)(1) because prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications that would establish incompatible standards for loanDepot. First loanDepot continues to maintain the PII of Nationwide Class members and other individuals, and varying adjudications could establish incompatible standards with respect to its duty to protect individuals' personal information; and whether the injuries suffered by Nationwide Class members are legally cognizable, among others. Prosecution of separate action by individual class members would also create a risk

of individual adjudications that would be dispositive of the interests of other class members not parties to the individual adjudications, or substantially impair or impede the ability of class members to protect their interests.

56. **Injunctive Relief:** In addition, Defendant has acted and/or refused to act on grounds that apply generally to the Nationwide Class, making injunctive and/or declaratory relief appropriate with respect to the class under Federal Rule of Civil Procedure 23(b)(2). Defendant continues to (1) maintain the personally identifiable information of Nationwide Class members, (2) fail to adequately protect their personally identifiable information, and (3) violate their rights under numerous state consumer protection laws and other claims alleged herein.

FIRST CAUSE OF ACTION

Negligence

(On Behalf of the Nationwide Class Against Defendant)

57. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

58. Plaintiff brings this claim on behalf of herself and the Nationwide Class.

59. Plaintiff and Nationwide Class members were required to provide Defendant with their PII. Defendant collected and stored this information including their names, Social Security numbers, payment card information, checking account and routing numbers, insurance provider information, salary information, dates of birth, addresses, and phone numbers.

60. Defendant had a duty to Plaintiff and Nationwide Class members to safeguard and protect their PII.

61. Defendant assumed a duty of care to use reasonable means to secure and safeguard this PII, to prevent its disclosure, to guard it from theft, and to detect any attempted or actual breach of its systems.

62. Defendant has full knowledge about the sensitivity of Plaintiff and Nationwide Class members' PII, as well as the type of harm that would occur if such

PII was wrongfully disclosed.

63. Defendant has a duty to use ordinary care in activities from which harm might be reasonably anticipated in connection with user PII data.

64. Defendant breached their duty of care by failing to secure and safeguard the PII of Plaintiff and Nationwide Class members. Defendant negligently stored and/or maintained its data security systems, and published that information on the Internet.

65. Further, Defendant by and through its above negligent actions and/or inactions, breached its duties to Plaintiff and Nationwide Class members by failing to design, adopt, implement, control, manage, monitor and audit its processes, controls, policies, procedures and protocols for complying with the applicable laws and safeguarding and protecting Plaintiff's and Nationwide Class members' PII within their possession, custody and control.

66. Defendant further breached their duty to Plaintiff and Nationwide Class members by failing to comply with the Consumers Legal Remedies Act, the Customer Record's Act, the Gramm-Leach-Bliley Act, and other state and federal laws designed to protect Plaintiff and Class members from the type of harm they here have suffered. Such a breach by Defendant constitutes negligence per se.

67. Plaintiff and the other Nationwide Class members have suffered harm as a result of Defendant's negligence. These victims' loss of control over the compromised PII subjects each of them to a greatly enhanced risk of identity theft, fraud, and myriad other types of fraud and theft stemming from either use of the compromised information, or access to their user accounts.

68. It was reasonably foreseeable – in that Defendant knew or should have known – that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Nationwide Class members' PII would result in its release and disclosure to unauthorized third parties who, in turn wrongfully used such PII, or disseminated it to other fraudsters for their wrongful use and for no lawful purpose.

69. But for Defendant's negligent and wrongful breach of their responsibilities and duties owed to Plaintiff and Nationwide Class members, their PII would not have been compromised.

70. As a direct and proximate result of Defendant's above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff's and Nationwide Class members' PII, they have incurred (and will continue to incur) the above-referenced economic damages, and other actual injury and harm for which they are entitled to compensation. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence/negligent misrepresentation.

71. Plaintiff and Nationwide Class members are entitled to injunctive relief as well as actual and punitive damages.

SECOND CAUSE OF ACTION

Violation of California Consumers Legal Remedies Act, California Civil Code § 1750, *et seq.*

(On Behalf of the Nationwide Class Against Defendant)

72. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

73. This cause of action is brought pursuant to the California Consumers Legal Remedies Act (the "CLRA"), California Civil Code § 1750, *et seq.* This cause of action does not seek monetary damages at this time and is limited solely to injunctive relief. Plaintiff will later amend this Complaint to seek damages in accordance with the CLRA after providing Defendant with notice required by California Civil Code § 1782.

74. Plaintiff and Nationwide Class Members are "consumers," as the term is defined by California Civil Code § 1761(d).

75. Plaintiff, Nationwide Class members, and Defendant has engaged in "transactions," as that term is defined by California Civil Code § 1761(e).

76. The conduct alleged in this Complaint constitutes unfair methods of competition and unfair and deceptive acts and practices for the purpose of the CLRA, and the conduct was undertaken by Defendant was likely to deceive consumers.

77. Defendant's conduct as described herein was and is in violation of the CLRA. Defendant's conduct violates at least the following enumerated CLRA provisions:

(a) in violation of § 1770(a) (2) Misrepresenting the source, sponsorship, approval, or certification of goods or services;

(b) in violation of § 1770(a)(5), representing that Defendant's "goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have";

(c) (b) in violation of § 1770(a)(7), represented that Defendant's "goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another";

(d) in violation of § 1770(a)(9), advertised goods or services with intent not to sell them as advertised";

(e) in violation of § 1770(a)(19), inserted an unconscionable provision in the contract"; and

(f) for other such violations of the CLRA that discovery will uncover.

78. Defendant violated these provisions by representing that they took appropriate measures to protect Plaintiff's and the Nationwide Class members' PII. Additionally, Defendant improperly handled, stored, or protected either unencrypted or partially encrypted data.

79. Defendant intentionally and knowingly misrepresented and omitted material facts regarding its data security practices and services with an intent to mislead Plaintiff and Class members.

80. Defendant's actions as described herein were done with conscious disregard of Plaintiff's rights and Defendant was wanton and malicious in

Defendant's concealment of the same.

81. In purchasing the services, Plaintiff and other Class members were deceived by Defendant's failure to disclose their knowledge of the deficient its data security practices and its services.

82. Plaintiff and other Class members had no way of knowing Defendant's representations were false, misleading, and incomplete or knowing the true nature of the its deficient data security practices and its services.

83. As alleged herein, Defendant engaged in a pattern of deception and public silence in the face of a known Defect.

84. Plaintiff and other Class members did not, and could not, unravel Defendant's deception on their own.

85. Defendant knew or should have known their conduct violated the CLRA.

86. Defendant owed Plaintiff and the Class members a duty to disclose the truth about the deficiencies in Defendant's data practices and its services and Defendant:

(a) Possessed exclusive knowledge of its security practices and its services;

(b) Intentionally concealed the foregoing from Plaintiff and Class members; and/or

(c) Made incomplete representations in advertisements and on its website, failing to warn the public of the deficiencies in its data security practices and its services.

87. Defendant had a duty to disclose to Plaintiff and the Class the deficiencies in its data security practices and its services to Plaintiff and the class members because the data security practices and its services left Plaintiff and Class' PII insecure and Plaintiff and the other Class members relied on Defendant's material misrepresentations and omissions regarding the features of its data security practices and its services.

88. Defendant's conduct proximately caused injuries to Plaintiff and the other

Class members that purchased the and suffered harm as alleged herein.

89. Plaintiff and the other Class members were injured and suffered ascertainable loss, injury-in-fact, and/or actual damage as a proximate result of Defendant's conduct in that Plaintiff and the other Class members, including: (a) theft of her valuable PII; (b) the imminent and certain impeding injury flowing from fraud and identity theft posed by their PII being placed in the hands of hackers; (c) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security – i.e., the difference in value between what Plaintiff should have received from Defendant when Defendant represented Plaintiff's PII would be protected by reasonable data security, and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect Plaintiff's PII; and (d) continued risk to Plaintiff's PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate an adequate measures to protect the PII that was entrusted to it.

90. As a direct and proximate result of Defendant's negligent acts of misfeasance and nonfeasance, Plaintiff and Class members have suffered and continue to suffer injury, including loss of time and productivity through efforts to ameliorate, mitigate, and deal with the future consequences of the Data Breach; theft of their valuable PII; and the imminent and certain impeding injury flowing from fraud and identity theft posed by their PII being placed in the hands of unauthorized third parties.

91. Defendant's failure to safeguard Plaintiff's and the Class's PII is particularly dangerous here where the exposed sensitive information includes social security numbers. According to Paige Schaffer, CEO of Generali Global Assistance's identity and digital protection services global unit, "where social security numbers are involved, victims' identity fraud risk remains elevated, if not for several years

then for life."[23]

92. Defendant's violations cause continuing injuries to Plaintiff and other Class members.

93. Defendant's unlawful acts and practices complained of herein affect the public interest.

94. Defendant knew of the deficient nature of its security practices related to its loan services and related services, and that its services were materially compromised by it.

95. The facts concealed and omitted by Defendant from Plaintiff and other Class members are material in that a reasonable consumer would have considered them to be important in deciding whether to enter into a loan with Defendant or pay a lower price for the loan.

96. As a result of engaging in such conduct, Defendant has violated Civil Code § 1770.

97. Had Plaintiff and the other Class members known about the deficiencies in Defendant's data security practices and its services, they would not have provided its PII to Defendant for purposes of entering into a loan with Defendant. As such, Plaintiff and Nationwide Class members were induced to enter into a relationship with Defendant and provide their PII.

98. Defendant's unfair and/or unlawful acts, practices, representations, omissions, and/or courses of conduct, as described herein, were undertaken by Defendant in a transaction intended to result in, and which did result in, the sale or lease of goods or services to consumers.

99. Pursuant to § 1780(d) of the CLRA, attached hereto as **Exhibit A** are the affidavits showing that this action has been commenced in the proper forum.

100. Pursuant to Cal. Civ. Code § 1780(a), Plaintiff seeks an order enjoining

[23] https://www.insurancebusinessmag.com/us/news/cyber/consumers-data-exposed-for-yearsfollowing-breach-incidents-178390.aspx.

Defendant from engaging in the methods, acts, or practices alleged herein, including further concealment of the deficient nature of its loan services as it relates to its data security practices related thereto.

101. Pursuant to Cal. Civ. Code § 1782(a)(2), Plaintiff demands judgment against Defendant under the CLRA for injunctive and equitable relief to enjoin the practices described herein.

102. Plaintiff intends to send a CLRA notice letter to Defendant certified mail, return receipt requested regarding Defendant's violations of the CLRA.

103. Pursuant to Cal. Civ. Code § 1782, if Defendant does not rectify its conduct within 30 days of the date of receipt of the letter, Plaintiff intends to amend this Complaint to add claims under the Cal. Civ. Code for Actual damages, but in no case shall the total award of damages in a class action be less than one thousand dollars ($1,000).

104. Under the CLRA, a plaintiff may without prior notification file a complaint alleging violations of the CLRA that seeks injunctive relief only. Then, if the Defendant does not remedy the CLRA violations within 30 days of notification, the plaintiff may amend her or his CLRA causes of action without leave of court to add claims for damages. Plaintiff, individually and on behalf of the class, intends to amend this complaint to add damages claims if Defendant does not remedy their respective violations as to Plaintiff and the Class Members within the statutory period.

105. Plaintiff has no adequate remedy at law for the future unlawful acts, methods, or practices as set forth above.

106. In bringing this action, Plaintiff has engaged the services of attorneys and has incurred reasonable legal fees and expenses in an amount to be proved at trial.

107. Plaintiff is thus entitled to recover Plaintiff's attorneys' fees, costs, and expenses.

108. Defendant's practices, acts, and courses of conduct in connection with the sale of its loan services that had deficient security, as described above, are likely to

mislead a reasonable consumer acting reasonably under the circumstances to his or her detriment. As a result of Defendant's acts and practices as alleged in this Complaint, Plaintiff is entitled to injunctive relief prohibiting Defendant from continuing in the future the unlawful, unfair, or fraudulent practice as described herein.

109. Plaintiff reasonably believed and/or depended on the material false and/or misleading information provided by, or omitted by, Defendant with respect to Defendant's unfair acts and deceptive practices.

110. By reason of the foregoing, Defendant's unlawful methods, acts, or practices as described herein have caused damage to Plaintiff, entitling Plaintiff to damages and injunctive relief; Attorneys' fees and costs; and other relief that this Court deems proper.

111. Plaintiff reserves the right to amend this Complaint and to assert a claim for damages pursuant to Civil Code §1782.

112. As a result, Plaintiff and Nationwide Class members were induced to enter into a relationship with Defendant and provide their PII.

113. Pursuant to Civil Code § 1780(a)(2) and (a)(5), Plaintiff seeks an order of this Court that includes, but is not limited to, an order enjoining Defendant from continuing to engage in unlawful, unfair, or fraudulent business practices or any other act prohibited by law.

114. Plaintiff and Nationwide Class members suffered injuries caused by Defendant's misrepresentations, because they provided their PII believing that Defendant would adequately protect this information.

115. Plaintiff and Nationwide Class members may be irreparably harmed and/or denied an effective and complete remedy if such an order is not granted.

116. The unfair and deceptive acts and practices of Defendant, as described above, present a serious threat to Plaintiff and members of the Nationwide Class.

THIRD CAUSE OF ACTION

Violation of Unfair Competition Law,

California Business and Professional Code Section 17200, *et seq*.

(On Behalf of the Nationwide Class Against Defendant)

117. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

118. Plaintiff brings this claim on behalf of herself and the Nationwide Class.

119. The California Unfair Competition Law, Cal. Bus. & Prof. Code §17200, *et seq*. ("UCL"), prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as defined by the UCL and relevant case law.

120. By reason of Defendant's above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized disclosure of Plaintiff and Nationwide Class members' PII, Defendant engaged in unlawful, unfair and fraudulent practices within the meaning of the UCL.

121. Defendant's business practices as alleged herein are unfair because they offend established public policy and are immoral, unethical, oppressive, unscrupulous and substantially injurious to consumers, in that the private and confidential PII of consumers has been compromised for all to see, use, or otherwise exploit.

122. Defendant's practices were unlawful and in violation of Civil Code § 1798 *et seq.* because Defendant failed to take reasonable measures to protect Plaintiff's and the Nationwide Class members' PII.

123. Defendant's business practices as alleged herein are fraudulent because they are likely to deceive consumers into believing that the PII they provide to Defendant will remain private and secure, when in fact it was not private and secure.

124. Plaintiff and the Nationwide Class members suffered (and continue to suffer) injury in fact and lost money or property as a direct and proximate result of Defendant's above-described wrongful actions, inactions, and omissions including, *inter alia*, the unauthorized release and disclosure of their PII.

125. Defendant's above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff's and Nationwide Class members' PII also constitute "unfair" business acts and practices within the meaning of Cal. Bus. & Prof. Code § 17200 *et seq*., in that Defendant's conduct was substantially injurious to Plaintiff and Nationwide Class members, offensive to public policy, immoral, unethical, oppressive and unscrupulous; the gravity of Defendant's conduct outweighs any alleged benefits attributable to such conduct.

126. But for Defendant's misrepresentations and omissions, Plaintiff and Nationwide Class members would not have provided their PII to Defendant or would have insisted that their PII be more securely protected.

127. As a direct and proximate result of Defendant's above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff and Nationwide Class members' PII, they have been injured: (1) the loss of the opportunity to control how their PII is used; (2) the diminution in the value and/or use of their PII entrusted to Defendant; (3) the compromise, publication, and/or theft of their PII; and (4) costs associated with monitoring their PII, amongst other things.

128. Plaintiff takes upon herself enforcement of the laws violated by Defendant in connection with the reckless and negligent disclosure of PII. There is a financial burden incurred in pursuing this action and it would be against the interests of justice to penalize Plaintiff by forcing him to pay attorneys' fees and costs from the recovery in this action. Therefore, an award of attorneys' fees and costs is appropriate under California Code of Civil Procedure § 1021.5.

FOURTH CAUSE OF ACTION

Violation of California Customer Records Act,

California Civil Code § 1798.80 et. seq.

(On Behalf of the Nationwide Class Against Defendant)

129. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

130. "[T]o ensure that personal information about California residents is protected," Civil Code section 1798.81.5 requires that any business that "owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

131. Defendant owns, maintains, and licenses personal information, within the meaning of section 1798.81.5, about Plaintiff and the Nationwide Class.

132. Defendant violated Civil Code section 1798.81.5 by failing to implement reasonable measures to protect Plaintiff and Nationwide Class members' personal information.

133. As a direct and proximate result of Defendant's violations of section 1798.81.5 of the California Civil Code, the Data Breach described above occurred.

134. As a direct and proximate result of Defendant's violations of section 1798.81.5 of the California Civil Code, Plaintiff and the Nationwide Class members suffered the damages described above including, but not limited to, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their personally identifying information.

135. Plaintiff and the Nationwide Class members seek relief under section 1798.84 of the California Civil Code including, but not limited to, actual damages, to be proven at trial, and injunctive relief.

FIFTH CAUSE OF ACTION

Breach of Contract

(On Behalf of the Nationwide Class Against Defendant)

136. Plaintiff re-alleges the paragraphs above as if fully set forth herein.

137. Plaintiff and Class members entered into a contract with Defendant for the provision of title insurance or other closing services.

138. The terms of Defendant's privacy policy are part of the contract.

139. Plaintiff and Class members performed substantially all that was required of them under their contract with Defendant, or they were excused from doing so.

140. Defendant failed to perform its obligations under the contract, including by failing to provide adequate privacy, security, and confidentiality safeguards for Plaintiff and Class member's information.

141. As a direct and proximate result of Defendant's breach of contract, Plaintiff and Class members did not receive the full benefit of the bargain, and instead received title insurance or other closing services that were less valuable than described in their contracts. Plaintiff and Class members, therefore, were damaged in an amount at least equal to the difference in value between that which was promised and Defendant's deficient performance.

142. Also, as a result of Defendant's breach of contract, Plaintiff and Class members have suffered actual damages resulting from the exposure of their personal information, and they remain at imminent risk of suffering additional damages in the future.

143. Accordingly, Plaintiff and Class members have been injured by Defendant's breach of contract and are entitled to damages and/or restitution in an amount to be proven at trial.

SIXTH CAUSE OF ACTION

Unjust Enrichment

(On Behalf of the Nationwide Class Against Defendant)

144. Plaintiff re-alleges the paragraphs above as if fully set forth herein.

145. Defendant received a benefit from Plaintiff and the Class in the form of payments for title insurance or other closing services.

146. The benefits received by Defendant were at Plaintiff's and the Class's

expense.

147. The circumstances here are such that it would be unjust for Defendant to retain the portion of Plaintiff's and the Class's payments that should have been earmarked to provide adequate privacy, security, and confidentiality safeguards for Plaintiff and Class members' personal information.

148. Plaintiff and the Class seek disgorgement of Defendant's ill-gotten gains.

SEVENTH CAUSE OF ACTION

Invasion of Privacy

(On Behalf of the Nationwide Class Against Defendant)

149. Plaintiff re-alleges the paragraphs above as if fully set forth herein.

150. Plaintiff brings this claim on behalf of himself and the Nationwide Class.

151. Plaintiff and Class members have a legally protected privacy interest in their PII that Defendant required them to provide and allow them to store.

152. Plaintiff and Class members reasonably expected that their PII would be protected and secured from unauthorized parties, would not be disclosed to any unauthorized parties or disclosed for any improper purpose.

153. Defendant unlawfully invaded the privacy rights of Plaintiff and Class members by (a) failing to adequately secure their PII from disclosure to unauthorized parties for improper purposes; (b) disclosing their PII to unauthorized parties in a manner that is highly offensive to a reasonable person; and (c) disclosing their PII to unauthorized parties without the informed and clear consent of Plaintiff and Class members. This invasion into the privacy interest of Plaintiff and Class members is serious and substantial.

154. In failing to adequately secure Plaintiff's and Class members' PII, Defendant acted in reckless disregard of their privacy rights. Defendant knew or should have known that their substandard data security measures are highly offensive to a reasonable person in the same position as Plaintiff and Class members.

155. Defendant violated Plaintiff's and Class members' right to privacy under

the common law as well as under state and federal law, including, but not limited to, the California Constitution, Article I, Section I.

156. As a direct and proximate result of Defendant's unlawful invasions of privacy, Plaintiff's and Class members' PII has been viewed or is at imminent risk of being viewed, and their reasonable expectations of privacy have been intruded upon and frustrated. Plaintiff and the proposed Class have suffered injury as a result of Defendant's unlawful invasions of privacy and are entitled to appropriate relief.

EIGHTH CAUSE OF ACTION

Breach of Implied Contract

(On Behalf of the Nationwide Class Against Defendant)

157. Plaintiff re-alleges the paragraphs above as if fully set forth herein.

158. Plaintiff and Class Members were required to provide their PII to Defendant as a condition of their use of Defendant's services. By providing their PII, and upon Defendant's acceptance of such information, Plaintiff and all Class Members, on one hand, and Defendant, on the other hand, entered into implied-in-fact contracts for the provision of data security, separate and apart from any express contracts.

159. These implied-in-fact contracts obligated Defendant to take reasonable steps to secure and safeguard Plaintiff's and other Class Members' PII. The terms of these implied contracts are further described in the federal laws, state laws, and industry standards alleged above, and Defendant expressly assented to these terms in their Privacy Policy and other public statement described above.

160. Plaintiff and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for services, along with Defendant's promise to protect their PII from unauthorized disclosure.

161. In their written Privacy Policy, loanDepot expressly promised Plaintiff and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

162. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide PII was Defendant 's obligation to (a) use such PII for business purposes only; (b) take reasonable steps to safeguard that PII; (c) prevent unauthorized disclosures of the PII; (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII; (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses; and (f) retain the PII only under conditions that kept such information secure and confidential.

163. Without such implied contracts, Plaintiff and Class Members would not have provided their PII to Defendant.

164. Plaintiff and Class Members fully performed their obligations under the implied contract with Defendant; however, Defendant did not.

165. Defendant breached the implied contracts with Plaintiff and Class Members by failing to reasonably safeguard and protect Plaintiff's and Class Members' PII, which was compromised as a result of the Data Breach.

166. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and other Class Members have suffered a variety of damages including but not limited to: the lost value of their privacy; they did not get the benefit of their bargain with Defendant; they lost the difference in the value of the secure lending services Defendant promised and the insecure services received; the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their lives, including, inter alia, that required to place "freezes" and "alerts" with credit reporting agencies, to contact financial institutions, to close or modify financial accounts, to closely review and monitor credit reports and various accounts for unauthorized activity, and to file police reports; and Plaintiff and other Class Members have been put at an increased risk of identity theft, fraud, and/or misuse of their PII, which may take months if not years to manifest, discover, and detect.

NINTH CAUSE OF ACTION

Breach of Fiduciary Duty

(On Behalf of the Nationwide Class Against Defendant)

167. Plaintiff re-alleges the paragraphs above as if fully set forth herein.

168. In light of their special relationship, Defendant has become the guardian of Plaintiff's and Class Members' PII and/ PHI. Defendant has become a fiduciary, created by its undertaking and guardianship of its customers' PII, to act primarily for the benefit of its customers, including Plaintiff and Class Members. This duty included the obligation to safeguard Plaintiff's and Class Members' PII and to timely notify them in the event of a data breach.

169. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its relationship. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to properly encrypt and otherwise protect the integrity of the system containing Plaintiff's and Class Members' PII.

170. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to (a) actual identity theft; (b) an increased risk of identity theft, fraud, and/or misuse of their PII; (c) the loss of the opportunity of how their PII is used; (d) the compromise, publication, and/or theft of their PII; (e) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (f) lost opportunity costs associated with the effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (g) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect customers' PII in their continued possession; and (h) future costs in terms of time, effort, and money that will be expended to prevent,

detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

171. As a direct and proximate result of Defendant's breach of their fiduciary duty, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

TENTH CAUSE OF ACTION

Injunctive/Declaratory Relief

(On Behalf of the Nationwide Class Against Defendant)

172. Plaintiff re-alleges the paragraphs above as if fully set forth herein.

173. This Count is brought under the federal Declaratory Judgment Act, 28 U.S.C. §2201.

174. As previously alleged, Plaintiff and Class Members entered into an implied contract that required Defendant to provide adequate security for the PII they collected from Plaintiff and Class Members.

175. Defendant owes a duty of care to Plaintiff and Class Members requiring them to adequately secure PII.

176. Defendant still possesses PII regarding Plaintiff and Class Members.

177. Since the Data Breach, Defendant has announced few if any changes to its data security infrastructure, processes or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent further attacks.

178. Members. In fact, now that Defendant's insufficient data security is known to hackers, the PII in Defendant's possession is even more vulnerable to cyberattack.

179. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff and Class Members are at risk of additional or further harm due to the exposure of their PII and Defendant's failure to

address the security failings that lead to such exposure.

180. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the Data Breach to meet Defendant's contractual obligations and legal duties.

181. Plaintiff, therefore, seeks a declaration (1) that Defendant's existing security measures do not comply with their contractual obligations and duties of care to provide adequate security, and (2) that to comply with their contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to, the following: a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors; b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring; c. Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures; d. Ordering that Defendant segment customer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems; e. Ordering that Defendant not transmit PII via unencrypted email; f. Ordering that Defendant not store PII in email accounts; g. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services; h. Ordering that Defendant conducts regular computer system scanning and security checks; i. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and j. Ordering Defendant to meaningfully educate their current, former, and prospective customers about the threats they face as a result of the loss of their PII to third parties, as well as

the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff requests that the Court enter a judgment awarding the following relief:

a. An order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Nationwide Class requested herein, appointing the undersigned as Class Counsel, and finding that Plaintiff is a proper representative of the Nationwide Class requested herein;

b. Injunctive relief requiring Defendant to (1) strengthen their data security systems that maintain personally identifying information to comply with the applicable state laws alleged herein (including, but not limited to, the California Customer Records Act) and best practices under industry standards; (2) engage third-party auditors and internal personnel to conduct security testing and audits on Defendant's systems on a periodic basis; (3) promptly correct any problems or issues detected by such audits and testing; and (4) routinely and continually conduct training to inform internal security personnel how to prevent, identify and contain a breach, and how to appropriately respond;

c. An order requiring Defendant to pay all costs associated with class notice and administration of class-wide relief;

d. Expressly excluding an award of damages under California's Consumer Legal Remedies Act ("CLRA") Cal. Civ. Code § 1750, an award to Plaintiff and all Nationwide Class members of compensatory, consequential, incidental, and statutory damages, restitution, and disgorgement, in an amount to be determined at trial;

e. An award to Plaintiff and all Nationwide Class members credit monitoring and identity theft protection services;

f. An award of attorneys' fees, costs, and expenses, as provided by law or equity;

g. An order requiring Defendant to pay pre-judgment and post-judgment

interest, as provided by law or equity; and

h. Such other or further relief as the Court may allow.

JURY TRIAL DEMANDED

Plaintiff demands a jury trial on all triable issues.

Dated: May 2, 2024

LAW OFFICE OF FRANCIS J. FLYNN, JR.

/s/Francis J. "Casey" Flynn, Jr.

Francis J. "Casey" Flynn, Jr. (SBN 304712)
6057 Metropolitan Plz.
Los Angeles, California 90036
Telephone: (314) 662-2836
casey@lawofficeflynn.com

LAW OFFICE OF PAUL C. WHALEN, P.C.
Paul C. Whalen (*pro hac vice forthcoming*)
768 Plandome Road
Manhasset, NY 11030
Telephone: (516) 426-6870
paul@paulwhalen.com

ATTORNEYS FOR PLAINTIFF AND THE PROPOSED CLASS